The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
1/14/2013

SUBJECT:
Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, the bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can likely be exploited if a user visits, or is redirected to a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Google Chrome versions prior to 24.0.1312.52

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Google Chrome, Details of these vulnerabilities are as follows:

- A use-after-free issue in the SVG layout. [CVE-2012-5145]
- A use-after-free issue in DOM handling. [CVE-2012-5147].
- A use-after-free issue when seeking video. [CVE-2012-5150]
- A use-after-free vulnerability when handling PDF fields.[CVE-2012-5156]
- A use-after-free issue in SVG filter handling. [CVE-2013-0832]
- An out-of-bounds read issue when seeking video. [CVE-2012-5152]
- An out-of-bounds issue during stack access in v8. [CVE-2012-5153]
- An out-of-bounds read vulnerability when handling a PDF image. [CVE-2012-5157]
- An out-of-bounds read issue related to printing. [CVE-2013-0833]
- An out-of-bounds read issue related to glyph handling. [CVE-2013-0834]
- An integer overflow vulnerability in audio IPC handling. [CVE-2012-5149]

- An integer overflow vulnerability in PDF JavaScript. [CVE-2012-5151]
- An integer overflow vulnerability in shared memory allocation. This issue only affects Windows. [CVE-2012-5154]
- A denial-of-service vulnerability occurs in browsers with geolocation. [CVE-2013-0835]
- A denial-of-service vulnerability exists in v8 garbage collection. [CVE-2013-0836]
- A denial-of-service vulnerability exists in extension tab handling. [CVE-2013-0837]
- A security-bypass vulnerability exists because of a same origin policy bypass with a malformed URL. [CVE-2012-5146]
- A security issue due to a missing filename sanitization in hyphenation support. [CVE-2012-5148]
- A security issue due to a missing Mac sandbox for worker processes. This issue only affects Mac. [CVE-2012-5155]
- A security vulnerability due to a bad cast when handling a PDF root. [CVE-2013-0828]
- A security vulnerability occurs due to tightened permissions on shared memory segments. [CVE-2013-0838]
- An incorrect file access vulnerability due to corrupt database metadata.
- A directory-traversal vulnerability when handling an extension process. [CVE-2013-0831]

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google here: http://support.google.com/chrome/bin/answer.py?hl=en&answer=95414
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

SecurityFocus:

http://www.securityfocus.com/bid/57251

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5145
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5148
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5149
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5150
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5151
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5152
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5153
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5154
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5155
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5156
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5157
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0828
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0829
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0830

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0831
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0832
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0833
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0834
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0835
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0836
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0837
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0838